US Government
Wireless Local Area Network (WLAN) Client
for
Basic Robustness Environments
Protection Profile

Version 1.0

November 2003

Table of Contents

List of Tables and Figures

Conventions and Terminology

Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP reader.

The notation, formatting, and conventions used in this PP are largely consistent with those used in version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP user.
The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP.
The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*.
The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment_value].
The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).
The **security target author** operation is used to denote points in which the final determination of attributes is left to the security target writer. Security target writer operations are indicated by the words "ST AUTHOR -".
The CC paradigm also allows protection profile and security target authors to create their own requirements. Such requirements are termed 'explicit requirements' and are permitted if the CC does not offer suitable requirements to meet the authors' needs. Explicit requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. In this PP, explicit requirements will be indicated with the "EXP" following the component name.
Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define "pass-fail" criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

NAMING CONVENTIONS

Assumptions: TOE security environment assumptions are given names beginning with "A."—e.g., A.ADMINISTRATION.

Threats: TOE security environment threats are given names beginning with "T."—e.g., T.SIGNAL_DETECT.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.GUIDANCE.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively,—e.g., O.ACCESS and OE.ADMIN.

Terminology

In the CC, Section 2.3 of Part 1 defines many terms. In addition to terms defined in the CC, this PP references the following defined terms.

Access -- Interaction between an entity and an object that results in the flow or modification of data.

Access Control -- Security service that controls the use of resources[1] and the disclosure and modification of data.[2]

Accountability -- Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator -- A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Assurance -- A measure of confidence that the security features of an IT system are sufficient to enforce its' security policy.

Asymmetric Cryptographic System -- A system involving two related transformations; one determined by a public key (the public transformation), and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).

Asymmetric Key -- The corresponding public/private key pair needed to determine the behavior of the public/private transformations that comprise an asymmetric cryptographic system.

Attack -- An intentional act attempting to violate the security policy of an IT system.

Authentication -- Security measure that verifies a claimed identity.

Authentication credentials -- Information used to verify a claimed identity.

Authorization -- Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized user -- An authenticated user who may, in accordance with the TSP, perform an operation.

[1] Hardware and software.
[2] Stored or communicated.

Availability -- Timely[3], reliable access to IT resources.

Compromise -- Violation of a security policy.

Confidentiality -- A security policy pertaining to disclosure of data.

Critical Security Parameters (CSP) -- Security-related information (e.g., cryptographic keys, authentication data such as passwords and pins, and cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Cryptographic boundary -- An explicitly defined contiguous perimeter that establishes the physical bounds (for hardware) or logical bounds (for software) of a cryptographic module.

Cryptographic key (key) -- A parameter used in conjunction with a cryptographic algorithm that determines [7]:

- the transformation of plaintext data into cipher text data,
- the transformation of cipher text data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data, or
- a digital authentication code computed from data.

Cryptomodule – This Protection uses the term "cryptomodule" in several cryptographic functional requirements. When used this term has very specific meaning. It describes:

- a cryptographic module that is FIPS 140-1/2 validated (to comply with FCS_BCM_EXP);
- the cryptographic functionality implemented in that module are FIPS-approved security functions that have been validated; and
- the cryptographic functionality is available in a FIPS-approved mode for the cryptomodule.

Cryptographic Module -- The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Cryptographic Module Security Policy -- A precise specification of the

[3] According to a defined metric.

security rules under which a cryptographic module must operate, including the rules derived from the requirements of this PP and additional rules imposed by the vendor.

Defense-in-Depth (DID) -- A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.

Discretionary Access Control (DAC) -- A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. These controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Embedded Cryptographic Module -- One that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system).

Enclave -- A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

Entity -- A subject, object, user, or another IT device, which interacts with TOE objects, data, or resources.

External IT entity -- Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Identity -- A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity -- A security policy pertaining to the corruption of data and TSF mechanisms.

Integrity label -- A security attribute that represents the integrity level of a subject or an object. Integrity labels are used by the TOE as the basis for mandatory integrity control decisions.

Integrity level -- The combination of a hierarchical level and an optional set of non-hierarchical categories that represent the integrity of data.

MAC Address -- Media Access Control Address, the globally unique 48 bit media layer address of a network device. Sometimes referred to as the physical address.

Mandatory Access Control (MAC) -- A means of restricting access to objects

based on subject and object sensitivity labels.[4]

Mandatory Integrity Control (MIC) -- A means of restricting access to objects based on subject and object integrity labels.

Multilevel -- The ability to simultaneously handle (e.g., share, process) multiple levels of data, while allowing users at different sensitivity levels to access the system concurrently. The system permits each user to access only the data to which they are authorized access.

Named Object[5] -- An object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user identities within the TSF.
- Subjects in the TOE must be able to request a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.

(Note: Due to the deletion of the last sentence in the OS PP (pertaining to intended use of the object being for sharing user data), something may need to be done to the requirements section of the PP (i.e., FDP_ACF) to ensure that some objects, which may satisfy the above but which are not intended for sharing user data do not need a full DAC implementation but rather it is acceptable if they are "owner only" or some other appropriate mechanism.)

Non-Repudiation -- A security policy pertaining to providing one or more of the following:

- To the sender of data, proof of delivery to the intended recipient,
- To the recipient of data, proof of the identity of the user who sent the data.

Object -- An entity within the TSC that contains or receives information and upon which subjects perform operations.

Operating Environment -- The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Operating System (OS) -- An entity within the TSC that causes operations to

[4] The Bell LaPadula model is an example of Mandatory Access Control
[5] The only named objects in this PP, are operating system controlled files.

be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies.

Operational key -- Key intended for protection of operational information or for the production or secure electrical transmissions of key streams.

Peer TOEs -- Mutually authenticated TOEs that interact to enforce a common security policy.

Public Object -- An object for which the TSF unconditionally permits all entities "read" access. Only the TSF or authorized administrators may create, delete, or modify the public objects.

Robustness -- A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DoD has three levels of robustness:

- **Basic:** Security services and mechanisms that equate to good commercial practices. Basic robustness equates to EAL-2 plus; ALC_FLR (Flaw Remediation), and AVA_MSU.1 (Misuse-Examination Guidance) as defined in CCIB-98-028, Part 3, Version 2.0

- **Medium:** Security services and mechanisms that provide for layering of additional safeguards above good commercial practices. Medium robustness equates to EAL-4 plus; ALC_FLR (Flaw Remediation); ADV_IMP.2; ADV_INT.1; ATE_DPT.2; and AVA_VLA.3 (Moderately Resistant Vulnerability Analysis) as defined in CCIB-98-028, Part 3, Version 2.0. If cryptographic functions are included in the TOE, then the PP should be augmented with AVA_CCA_EXP.2 as documented in the Protection Profile Medium Robustness Consistency Guidance.

- **High:** Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

Secure State -- Condition in which all TOE security policies are enforced.

Security attributes -- TSF data associated with subjects, objects, and users that is used for the enforcement of the TSP.

Security level -- The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity on the information [10].

Sensitivity label -- A security attribute that represents the security level of an object and that describes the sensitivity (e.g. Classification) of the data in the

object. Sensitivity labels are used by the TOE as the basis for mandatory access control decisions [10].

Split key -- A variable that consists of two or more components that must be combined to form the operational key variable. The combining process excludes concatenation or interleaving of component variables.

Subject -- An entity within the TSC that causes operations to be performed.

Symmetric key -- A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.

Threat -- Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent - Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.

TOE Security Function (TSF) Data -- Information used by the TSF in making TOE security policy (TSP) decisions. TSF data may be influenced by users if allowed by the TSP. Security attributes, authentication data, and access control list entries are examples of TSF data.

Unauthorized User -- Any person who is not authorized, under the TSP, to access the TOE. This definition authorized users who seek to exceed their authority.

User -- Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User Data -- Data created by and for the authorized user that does not affect the operation of the TSP. User data is separate from the TSF data, which has security attributes associated with it and the system data.

Vulnerability -- A weakness that can be exploited to violate the TOE security policy.

Wireless Client -- An device consisting of hardware and software used to provide a wirelessly interface to communicate with an with other wireless devices.

Document Organization

Section 1 provides the introductory material for this PP. It includes an introduction, a brief description of the WLAN client TOE and additional identifying information. It also includes a discussion of the factors used to define the TOE environment and the level of Robustness selected for this PP.

Section 2 describes, in detail, the WLAN client TOE (i.e., the TOE for this PP) and the IT environment upon which the TOE depends.

Section 3 describes the TOE security environment. This includes

- Secure-use assumptions that describe the presumptive conditions for secure use of the TOE in the a basic robustness environment
- Threats that are to be addressed by either completely or partially by the technical countermeasures implemented in the WLAN client.
- Organizational policies that levy further requirements on the TOE.

In addition this section also identifies those threats and policies that are defined as part of the basic robustness environment that the WLAN client does not address

Section 4 defines the security objectives for the WLAN client in a basic robustness environment.

Section 5 contains the functional and assurance requirements derived from the CC, Parts 2 and 3, respectively that must be satisfied by the WLAN client. This section also identifies requirements that are levied on the TOE IT environment.

Section 6 provides a rationale to demonstrate that the information technology security objectives for the TOE and its IT environment satisfy the identified policies and threats. The section then provides rationale to show that the set of requirements are sufficient to meet each objective, and that each security objective is addressed by one or more component requirements. Therefore, the two aforementioned subsections provide arguments that the security objectives and security requirements are both necessary and sufficient, respectively and collectively, to meet the needs dictated by the policies and threats. Section also 6 provides arguments that to address any unsatisfied dependencies, and the selected strength of function.

Section 7, Identifies references to noteworthy background and/or supporting materials.

Appendix A is an acronym list that defines frequently used acronyms.

1. Introduction

This Protection Profile (PP) supports future Department of Defense (DoD) procurements of commercial off-the-shelf (COTS) wireless local area network (WLAN) clients that will be used in basic robustness environments. This PP details the policies, assumptions, threats, security objectives, security functional requirements, and security assurance requirements for the WLAN client and its supporting environment. In the case of this PP, the TOE supporting environment is significant. The TOE is a wireless network interface card. This device is relatively simple and is a component of a larger system. As such, the TOE must rely heavily on the TOE IT environment for protection.

This PP has two primary audiences: Information System Security Engineers (ISSE) and COTS WLAN client product vendors. The ISSE may use this PP to help in designing and assessing installations in which COTS WLAN clients are part of the information system. WLAN client product vendors will use the PP to learn the DoD security requirements for new COTS WLANs being procured.

1.1 Identification

Title:	US Government Wireless Local Area Network (WLAN) Client for Basic Robustness Environments Protection Profile.
Version:	0.90
Sponsor:	National Security Agency (NSA)
CC Version:	Common Criteria (CC) Version 2.1, and applicable interpretations.
Evaluation Level:	Evaluation Assurance Level (EAL) 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of Guidance).
Keywords:	radio, basic assurance, wireless, network, wireless local area network, wireless LAN, WLAN, LAN

1.2 Protection Profile Overview

This PP specifies the DoD's information security needs for a Basic Robustness WLAN Client. It is expected that the wireless client will be a component in a larger system (for example, a wireless card installed in a laptop computer). This PP requires privacy and integrity of communications over the WLAN using commercially available cryptographic algorithms. Security administration is the responsibility of the user of each component (i.e., client). The assurance requirements specified in the PP are EAL 2 augmented with flaw remediation, assurance maintenance and misuse analysis

1.3 TOE Environment Defining Factors

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: **value of the resources** and **authorization of the entities** to those resources.

In general terms, the environment for a TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).

Note that there are an infinite number of combinations of entity authorization and value of resources; this conceptually "makes sense" because there are an infinite number of potential environments, depending on how the resources are valued by the organization, and the variety of authorizations the organization defines for the associated entities. In the next section 1.2.2, these two environmental factors will be related to the robustness required for selection of an appropriate TOE.

1.3.1 Value of Resources

Value of the resources associated with the TOE includes the data being processed or used by the TOE, as well as the TOE itself (for example, a real-time control processor). "Value" is assigned by the using organization. For example, in the DoD low-value data might be equivalent to data marked "FOUO", while high-value data may be those classified Top Secret. In a commercial enterprise, low-value data might be the internal organizational structure as captured in the corporate on-line phone book, while high-value data might be corporate research results for the next generation product. Note that when considering the value of the data one must also consider the value of data or resources that are accessible through exploitation of the TOE. For example, a firewall may have "low value" data itself, but it might protect an enclave with high value data. If the firewall was being depended upon to protect the high value data, then it must be treated as a high-value-data TOE.

1.3.2 Authorization of Entities

Authorization that entities (users, administrators, other IT systems) have with respect to the TOE (and thus the resources of that TOE, including the TOE itself) is an abstract concept reflecting a combination of the trustworthiness of an entity and the access and privileges granted to that entity with respect to the resources of the TOE. For instance, entities that have total authorization to all data on the TOE are at one end of this spectrum; these entities may have privileges that allow them to read, write, and modify anything on the TOE, including all TSF data. Entities at the other end of the spectrum are those that are authorized to few or no TOE resources. For example, in the case of a router, non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources. In the case of an OS, an entity

may not be allowed to log on to the TOE at all (that is, they are not valid users listed in the OS's user database)**.**

It is important to note that authorization **does not** refer to the **access** that the entities actually have to the TOE or its data. For example, suppose the owner of the system determines that no one other than employees was authorized to certain data on a TOE, yet they connect the TOE to the Internet. There are millions of entities that are not **authorized** to the data (because they are not employees), but they actually have connectivity to the TOE through the Internet and thus can attempt to access the TOE and its associated resources.

Entities are characterized according to the value of resources to which they are authorized; the extent of their authorization is implicitly a measure of how trustworthy the entity is with respect to compromise of the data (that is, compromise of any of the applicable security policies; e.g., confidentiality, integrity, availability). In other words, in this model the greater the extent of an entity's authorization, the more trustworthy (with respect to applicable policies) that entity is.

1.3.3 Selection Of Appropriate Robustness Levels

Robustness is a characteristic of a TOE defining how well it can protect itself and its resources; a more robust TOE is better able to protect itself. This section relates the defining factors of IT environments, authorization, and value of resources to the selection of appropriate robustness levels.

When assessing any environment with respect to Information Assurance the critical point to consider is the likelihood of an attempted security policy compromise, which was characterized in the previous section in terms of entity authorization and resource value. As previously mentioned, robustness is a characteristic of a TOE that reflects the extent to which a TOE can protect itself and its resources. It follows that as the likelihood of an attempted resource compromise increases, the robustness of an appropriate TOE should also increase.

It is critical to note that several combinations of the environmental factors will result in environments in which the likelihood of an attempted security policy compromise is similar. Consider the following two cases:

The first case is a TOE that processes only low-value data. Although the organization has stated that only its employees are authorized to log on to the system and access the data, the system is connected to the Internet to allow authorized employees to access the system from home. In this case, the least trusted entities would be unauthorized entities (e.g. non-employees) exposed to the TOE because of the Internet connectivity. However, since only low-value data are being processed, the likelihood that unauthorized entities would find it worth their while to attempt to compromise the data on the system is low and selection of a basic robustness TOE would be appropriate.

The second case is a TOE that processes high-value (e.g., classified) information. The organization requires that the TOE be stand-alone, and that every user with physical and logical access to the TOE undergo an investigation so that they are authorized to the highest value data on the TOE. Because of the extensive checks done during this investigation, the organization is assured that only highly trusted users are authorized to use the TOE. In this case, even though high value information is being processed, it is unlikely that a compromise of that data will be attempted because of the authorization and trustworthiness of the users and once again, selection of a basic robustness TOE would be appropriate.

The preceding examples demonstrated that it is possible for radically different combinations of entity authorization/resource values to result in a similar likelihood of an attempted compromise. As mentioned earlier, the robustness of a system is an indication of the protection being provided to counter compromise attempts. Therefore, a basic robustness system should be sufficient to counter compromise attempts where the likelihood of an attempted compromise is low. The following chart depicts the "universe" of environments characterized by the two factors discussed in the previous section: on one axis is the authorization defined for the least trustworthy entity, and on the other axis is the highest value of resources associated with the TOE.

As depicted in the following figure, the robustness of the TOEs required in each environment steadily increases as one goes from the upper left of the chart to the lower right; this corresponds to the need to counter increasingly likely attack attempts by the least trustworthy entities in the environment. Note that the shading of the chart is intended to reflects the notion that different environments engender similar levels of "likelihood of attempted compromise", signified by a similar color. Further, the delineations between such environments are not stark, but rather are finely grained and gradual.

While it would be possible to create many different "levels of robustness" at small intervals along the "Increasing Robustness Requirements" line to counter the increasing likelihood of attempted compromise due to those attacks, it would not be practical nor particularly useful. Instead, in order to implement the robustness strategy where there are only three robustness levels: Basic, Medium, and High, the graph is divided into three sections, with each section corresponding to set of environments where the likelihood of attempted compromise is roughly similar. This is graphically depicted in the following chart.

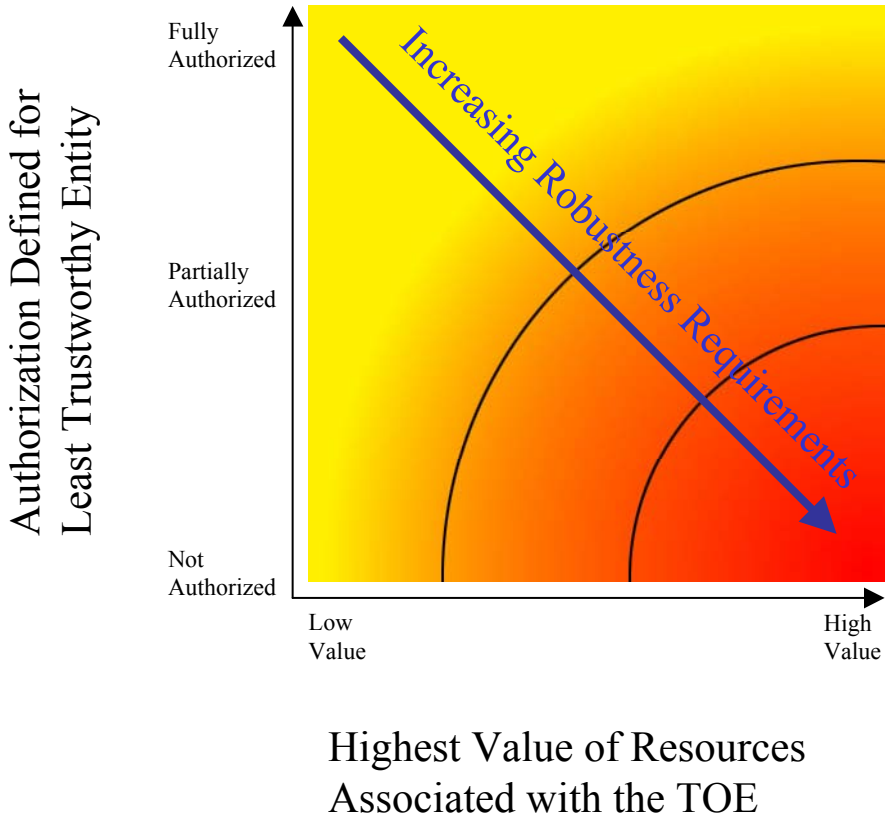

Figure 1: Value of TOE Resources vs. Trust

In this second representation of environments and the robustness plane below, the "dots" represent given instantiations of environments; like-colored dots define environments with a similar likelihood of attempted compromise. Correspondingly, a TOE with a given robustness should provide sufficient protection for environments characterized by like-colored dots. In choosing the appropriateness of a given robustness level TOE PP for an environment, then, the user must first consider the lowest authorization for an entity as well as the highest value of the resources in that environment. This should result in a "point" in the chart above, corresponding to the likelihood that that entity will attempt to compromise the most valuable resource in the environment. The appropriate robustness level for the specified TOE to counter this likelihood can then be chosen.

The difficult part of this activity is differentiating the authorization of various entities, as well as determining the relative values of resources; (e.g., what constitutes "low value" data vs. "medium value" data). Because every organization will be different, a rigorous definition is not possible. In section 3 of this PP, the targeted threat level for a basic robustness TOE is characterized. This information is provided to help organizations using this PP insure that the functional requirements specified by this basic robustness PP are appropriate for their intended application of a compliant TOE.

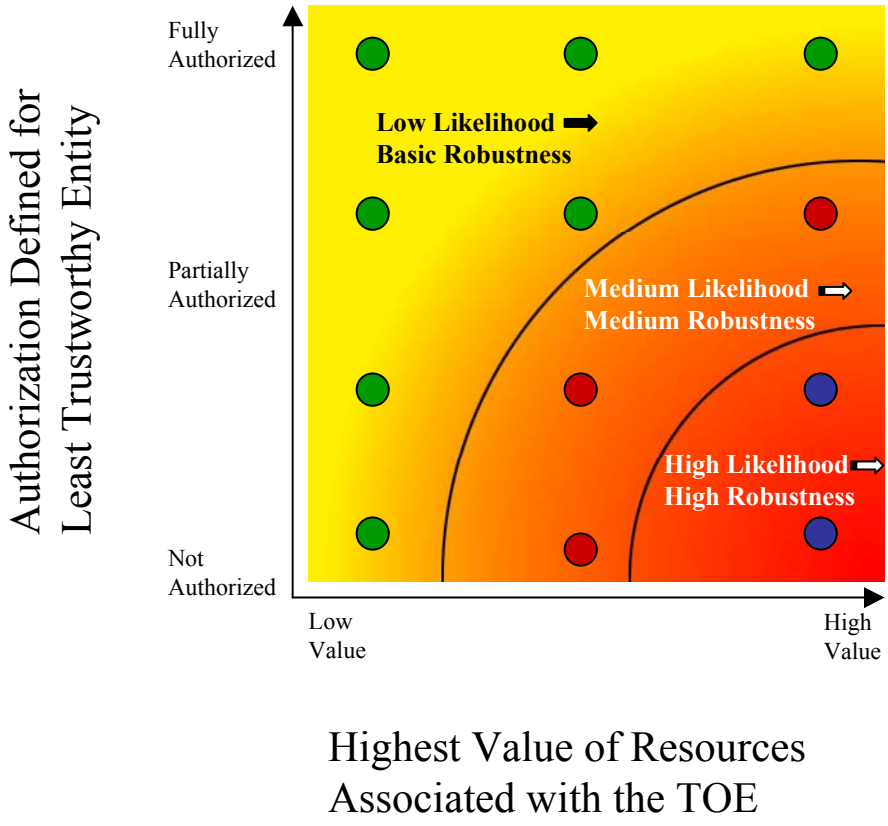

Figure 2: Value of TOE Resources vs. Robustness

1.4 Related Protection Profiles

US Government Wireless Access System for Basic Robustness Environments Protection Profile [1].

This Profile supersedes the Peer-to-Peer Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments Protection Profile, Version .6, dated September 28, 2001.

2. TOE Description

The Target of Evaluation (TOE) is a WLAN client. It is expected that the client will be a component of a larger system (e.g. the WLAN client will be installed on a laptop computer). For the purpose of this PP we will be discussing a typical wired to wireless configuration. However the reader should keep in mind that it does not preclude any other wireless configuration that may exist. This PP does not dictate a particular configuration. Instead the PP addresses the security requirements for the client that provides communication between the wireless user and the wired network and its resources. The security requirements of the TOE are administration, audit, and encryption.

A WLAN is an extension, or possibly a replacement, of a traditional wired network. The WLAN client is in most cases installed into the laptop or mobile device. Therefore, it must also be understood that the TOE alone does not provide all of the security functionality that is required in a Basic Robustness Environment. A traditional wireless LAN is set up as in Figure 3. In the typical configuration, the client and access system establish a connection through which all data will traverse to the wired side of the network. As such, it is not intended to provide any direct network services to the users that connect through the access system. The client will rely mainly on the environment in which it resides to perform many of the management duties and providing secure access to the network.

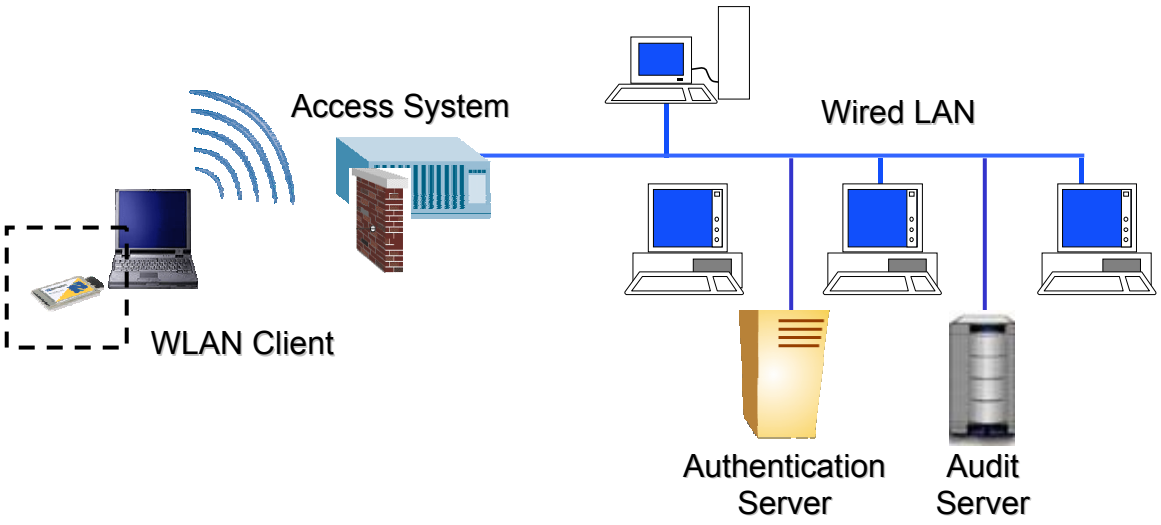

Figure 3: Example of WLAN architecture with the WLAN client

Table 3 identifies threats and policies that are expected to exist in a Basic Robustness Environment that the WLAN client TOE does not address. Similarly Table 7 identifies security objectives for the environment that must be addressed either by assumptions or requirements levied on the TOE IT environment.

While this document does not dictate vendor implementations of the functional and assurance requirements defined in Section 5, it does require that the wireless card, any device drivers necessary to operate the TOE as part of the larger system, and any management software that is used to install, configure or operate the WLAN client be included as part of the TOE in any Security Targets (ST) claiming conformance to this PP.

2.1 Administration

"Administrator" refers to the roles assigned to the individual(s) responsible for the installation, configuration, and maintenance of the TOE. Since this TOE is part of a larger system, it is expected that those responsible for administration of the TOE IT environment will also be responsible for TOE administration. This PP does not preclude multiple separate administrative roles but requires only a single administrator for the TOE.

2.2 Encryption

This TOE includes requirements for cryptographic modules. Those modules must comply with Federal Information Processing Standard Publication (FIPS PUB) 140-1/2, which defines security requirements for cryptographic modules. A cryptographic module is that part of a system or application that provides cryptographic services, such as encryption, authentication, or electronic signature generation and verification. Products and systems compliant with this PP are expected to utilize cryptographic modules compliant with this FIPS PUB.

2.3 Audit

This TOE is expected to be a component in a larger computing platform. As such its responsibilities with respect to audit are limited to the generation of audit events. It is expected that the TOE IT environment will provide the mechanisms for audit event storage and retrieval.

2.4 TOE IT Environment

The hardware platform (e.g., handheld PC, notebook computer) in which the WLAN client is installed and the operating system are not required to be included as part of the TOE at basic robustness. However, since the TOE is expected to be part of a larger IT system, it may be necessary for the TOE rely upon that IT environment to augment the

protections offered by the TOE. The specific requirements for the IT environment are identified in section 5.3.

3. TOE Security Environment

The WLAN client specified within this PP is intended for a basic robustness environment. Basic robustness TOEs falls in the upper left area of the previously discussed robustness figures. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.

Threat agent motivation can be considered in a variety of ways. One possibility is that the value of the data process or protected by the TOE will generally be seen as of little value to the adversary (i.e., compromise will have little or no impact on mission objectives). Another possibility, (where higher value data is processed or protected by the TOE) is that procuring organizations will provide other controls or safeguards (i.e., controls that the TOE itself does not enforce) in the fielded system in order to increase the threat agent motivation level for compromise beyond a level of what is considered reasonable or expected to be applied.

In a basic robustness environment, users are trusted to neither attempt malicious attacks nor by-pass access control measures. Users are also trusted to correctly apply the organization's security policies. The TOE is not expected to protect against sophisticated, technical attack.

Chapter 3 describes the assumptions, threats, and policies that are relevant to both the TOE and the WLAN TOE environment. The first section describes the secure usage assumptions, which are those items that the TOE itself cannot implement or enforce. The next section covers the threats that are expected to exist in a basic robustness environment. The final section discusses the DoD policies relevant to the operation of a WLAN client in a basic robustness environment.

3.1 Secure Usage Assumptions

Assumptions are non-IT items that the TOE itself cannot implement or enforce. Table 1 identifies the assumptions for the WLAN client in the operational environment.

Table 1: TOE Assumptions

Name	Assumption

A.BASIC_ROBUSTNESS_IT_ ENVIRONMENT[6]	The TOE is a Wireless LAN card and is expected to be installed in an IT environment (e.g. PC hardware and O/S) that can appropriately address those threats and policies identified in "Table 3: Basic Robustness Threats NOT Applicable to the TOE" and meets the IT environmental requirements necessary to support the correct operation of the TOE.
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.

3.2 Threats to Security

In addition to helping define the robustness appropriate for a given environment, the threat agent is a key component of the formal threat statements in the PP. Threat agents are typically characterized by a number of factors such as *expertise*, *available resources*, and *motivation*. Because each robustness level is associated with a variety of environments, there are corresponding varieties of specific threat agents (that is, the threat agents will have different combinations of motivation, expertise, and available resources) that are valid for a given level of robustness. The following discussion explores the impact of each of the threat agent factors on the ability of the TOE to protect itself (that is, the robustness required of the TOE).

The *motivation* of the threat agent seems to be the primary factor of the three characteristics of threat agents outlined above. Given the same expertise and set of resources, an attacker with low motivation may not be as likely to attempt to compromise the TOE. For example, an entity with no authorization to low value data none-the-less has low motivation to compromise the data; thus a basic robustness TOE should offer sufficient protection. Likewise, the fully authorized user with access to highly valued data similarly has low motivation to attempt to compromise the data, thus again a basic robustness TOE should be sufficient.

Unlike the motivation factor, however, the same can't be said for *expertise*. A threat agent with low motivation and low expertise is just as unlikely to attempt to compromise a TOE as an attacker with low motivation and high expertise; this is because the attacker with high expertise does not have the motivation to compromise the TOE even though

[6] This Assumption has been included in the WLAN Client PP in order to ensure that the operational environment in which the TOE is used can address basic robustness threat and policies not addressed by the TOE. It must not be construed as allowing the TOE environment to satisfy TOE functional requirements.

they may have the expertise to do so. The same argument can be made for *resources* as well.

Therefore, when assessing the robustness needed for a TOE, the motivation of threat agents should be considered a "high water mark". *That is, the robustness of the TOE should increase as the motivation of the threat agents increases.*

Having said that, the relationship between expertise and resources is somewhat more complicated. In general, if resources include factors other than just raw processing power (money, for example), then expertise should be considered to be at the same "level" (low, medium, high, for example) as the resources because money can be used to purchase expertise. Expertise in some ways is different, because expertise in and of itself does not automatically procure resources. However, it may be plausible that someone with high expertise can procure the requisite amount of resources by virtue of that expertise (for example, hacking into a bank to obtain money in order to obtain other resources).
It may not make sense to distinguish between these two factors; in general, it appears that the only effect these may have is to lower the robustness requirements. For instance, suppose an organization determines that, because of the value of the resources processed by the TOE and the trustworthiness of the entities that can access the TOE, the motivation of those entities would be "medium". This normally indicates that a medium robustness TOE would be required because the likelihood that those entities would attempt to compromise the TOE to get at those resources is in the "medium" range. However, now suppose the organization determines that the entities (threat agents) that are the least trustworthy have no resources and are unsophisticated. In this case, even though those threat agents have medium motivation, the likelihood that they would be able to mount a successful attack on the TOE would be low, and so a basic robustness TOE may be sufficient to counter that threat.

It should be clear from this discussion that there is no "cookbook" or mathematical answer to the question of how to specify exactly the level of motivation, the amount of resources, and the degree of expertise for a threat agent so that the robustness level of TOEs facing those threat agents can be rigorously determined. However, an organization can look at combinations of these factors and obtain a good understanding of the likelihood of a successful attack being attempted against the TOE. Each organization wishing to procure a TOE must look at the threat factors applicable to their environment; discuss the issues raised in the previous paragraph; consult with appropriate accreditation authorities for input; and document their decision regarding likely threat agents in their environment.

The important general points we can make are:

- The motivation for the threat agent defines the upper bound with respect to the level of robustness required for the TOE
- A threat agent's expertise and/or resources that is "lower" than the threat agent's motivation (e.g., a threat agent with high motivation but little expertise and few resources) may lessen the robustness requirements for the TOE (see next point, however).

- The availability of attacks associated with high expertise and/or high availability of resources (for example, via the Internet or "hacker chat rooms") introduces a problem when trying to define the expertise of, or resources available to, a threat agent.

The threats listed in Table 2 are general. Exposure of wireless communications in the RF transmission environment introduces unique threats to the WLAN client. With WLANs, an adversary no longer requires physical access to the network in order to exploit a wireless system. The WLAN is susceptible to over-the-air signal intercept, spoofing, and jamming attacks. Given the nature of the basic robustness environment, the threats identified exclude those that would be considered a sophisticated attack (i.e., intentional jamming, traffic analysis).

Table 2: Threats

Threat Name	Threat Definition
T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.ACCIDENTAL_CRYPTO_COMPROMISE	A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through

Threat Name	Threat Definition
	reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).

In the case of a WLAN client device, the TOE is a component of a larger system and as such, does not address all of the threats identified as part of a typical basic robustness environment. Table 3 identifies those threats not addressed by the TOE.

Table 3: Basic Robustness Threats NOT Applicable to the TOE

Threat Name	Threat Definition	Rationale for NOT Including this Threat
T.AUDIT_COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As a component of a larger system, the TOE is responsible for generating audit records in accordance with the audit policy specified by the system administrator. It is expected that these records will be stored outside of the TOE. The TOE IT environment will provide appropriate mechanisms to protect audit records after they have been generated.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As a component of a larger system, the TOE (wireless NIC) is not provided with user or process identification information and is not expected to prevent masquerading by an unauthorized user or process. It is also important to note that although the TOE does include a MAC address filtering policy,

Threat Name	Threat Definition	Rationale for NOT Including this Threat
		the TOE itself cannot verify that the MAC address of the IT entity with which is communicating. Therefore, this threat is not addressed by the TOE.
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.	The PP authors recognize that this threat, although appropriate for a basic robustness environment, but that it will not be addressed (either fully or partially) by the TOE. The TOE, in this case, is a wireless network interface card, which is installed as part of a larger system. As a component of larger system, the only unattended sessions within the TOE scope of control are network connections. The PP authors believe that this threat is more appropriately mitigated by the operating system in which the WLAN client is installed. The OS is capable of uniformly enforcing a policy for unattended network, serial interface and console sessions.
T.UNAUTHORIZED_ ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As a component of a larger system, the does not have access to information identifying authorized or unauthorized users.
T.UNIDENTIFIED_ ACTIONS	The administrator may not have the ability to notice potential security violations, thus limiting the administrator's	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As a component of a larger system, the TOE is responsible for generating audit records in accordance with the

Threat Name	Threat Definition	Rationale for NOT Including this Threat
	ability to identify and take action against a possible security breach.	audit policy specified by the system administrator. However the TOE is not expected to provide facilities to either store or review audit records. It is expected that the TOE IT environment will provide facilities to review, sort, select and other manage the audit records.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 4 identifies the organizational security policies applicable to the basic robustness WLAN client. PP-compliant TOEs must address the organizational security policies described below.

Table 4: Organizational Security Policies

Policy Name	Policy Definition
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

In the case of a WLAN client device, the TOE is a component of a larger system and as such, does not address all of the policies identified as part of a basic robustness environment. Table 5 identifies those policies.

Table 5: Basic Robustness Policies Not Addressed By the TOE

Policy Name	Policy Definition	Rationale for NOT Including this Policy
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	As is noted previously, this TOE is a wireless network interface card, which is installed as part of a larger system. As such, the TOE IT environment (e.g. operating system) is responsible for the display of appropriate banner information.

3.4 Security Function Policies

Several of the functional requirements in section 5.1 reference Security Function Policies (SFPs). SFPs are named pieces of requirements. They are not organizational policies. Each SFP is listed in the table below with an explanation that supplies additional information and interpretation.

Table 5: Security Function Policies

Policy Name	Policy Definition
P.WIRELESS ENCRYPTION SFP	The users/access system administrators shall specify that the TOE encrypt/decrypt user data as it transits to/from wireless network.

4. Security Objectives for the TOE

Table 6 identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified.

Table 6: Security Objectives for the TOE

Name	TOE Security Objective	Corresponding Threats or Policies
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.	T.ACCIDENTAL_ADMIN_ ERROR
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events.	P.ACCOUNTABILITY
O.CONFIGURATION_ IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.	T.POOR_DESIGN, T.POOR_IMPLEMENTATION
O.CORRECT_ TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	T.POOR_TEST
O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-1/2 validated cryptographic services.	P.CRYPTOGRAPHY, T.CRYPTO_COMPROMISE
O.DOCUMENTED_ DESIGN	The design of the TOE is adequately and accurately documented.	T.POOR_DESIGN

Name	TOE Security Objective	Corresponding Threats or Policies
O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE.	T.TSF_COMPROMISE
O.PARTIAL_ FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	T.POOR_IMPLEMENTATION, T.POOR_TEST
O.RESIDUAL_ INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	T.RESIDUAL_DATA, T.TSF_COMPROMISE, P.CRYPTOGRAPHY, T.CRYPTO_COMPROMISE
O.VULNERABILITY_ ANALYSIS	The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	T.POOR_DESIGN, T.POOR_IMPLEMENTATION, T.POOR_TEST

4.1 Security Objectives for the Environment

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 7 identifies the security objectives for the environment.

Table 7: Security Objectives for the Environment

Name	TOE Security Objective	Corresponding Assumption, Threat, or Policy

Name	TOE Security Objective	Corresponding Assumption, Threat, or Policy
OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	T.TSF_COMPROMISE, P.ACCOUNTABILITY
OE.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.	A.NO_EVIL
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.	A.PHYSICAL
OE.RESIDUAL_ INFORMATION	The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	T.RESIDUAL_DATA
OE.SELF_ PROTECTION	The TOE IT environment will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through its their interfaces.	T.TSF_COMPROMISE, T.CRYPTO_COMPROMISE
OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	P.ACCOUNTABILITY
OE.TOE_ACCESS	The TOE IT environment will provide mechanisms that control a user's logical access to the TOE.	P.ACCOUNTABILITY

5. IT Security Requirements

This section provides functional and assurance requirements that must be satisfied by a PP-compliant TOE. These requirements consist of functional components from Part 2 of the Common Criteria (CC) and an EAL containing assurance components from Part 3 of the CC.

5.1.1 Strength of Function Claims

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism, except for cryptographic functions. In the case of this PP, this minimum level shall be SOF-basic.

5.1.2 Identification of Standards Compliance Methods

For this PP, cryptographic operations and key management functions must meet FIPS 140-1/2 (Level 1). The designated approval authority of the TOE-user organization will specify the methodology used to show compliance to FIPS 140-1/2 standards. Authorized certificates used by a PP-compliant TOE must be DoD PKI Class 3 or 4, X.509 certificates.

5.1.3 TOE Security Functional Requirements

The SFRs for the TOE consist of the following components from Part 2 of the CC, summarized in Table 8. All dependencies among the SFRs are satisfied by the inclusion of the relevant requirement within the TOE security requirements.[7]

5.2 SECURITY FUNCTIONAL REQUIREMENTS

This section provides information related to the TOE's Security Functional Requirements (SFR). The first subsection addresses strength of function claims. The second subsection identifies standards compliance methods for the cryptographic SFRs included in this PP. The third subsection specifies the SFRs.

Table 8: TOE Security Functional Requirements

Functional Component		Dependencies
FAU_GEN.1-NIAP-0410	Audit Data Generation	FPT_STM.1
FCS_BCM_EXP.1	Explicit: Baseline Cryptographic Module	None

[7]Not all of the dependencies identified are satisfied. Section 6 provides the rationale unsatisfied dependencies.

Functional Component		Dependencies
FCS_CKM_EXP.2	Explicit: Cryptographic Key Handling and Storage	FDP_ITC.1 - Or - FCS_COP_EXP.1; FCS_CKM.1; FCS_CKM.4; FMT_MSA.2
FCS_CKM.4	Cryptographic Key Destruction	None
FCS_COP_EXP.1	Explicit: Random Number Generation	FDP_ITC.1 - Or - FCS_CKM.1; FCS_CKM.4; FMT_MSA.2
FCS_COP_EXP.2	Explicit: Cryptographic Operation (AES data encryption/decryption)	FDP_ITC.1 - Or - FCS_CKM.1; FCS_CKM.4; FMT_MSA.2
FDP_IFC.1	Subset information flow control (Wireless Encryption Policy)	FDP_IFF.1 FMT_MSA.3
FDP_IFF.1-NIAP-0407	Simple Security Attributes (Wireless Encryption Policy)	FDP_IFC.1
FDP_RIP.1	Subset Residual Information Protection	None
FMT_SMF.1(1)	Specification of Management Functions (Cryptographic Function)	None
FMT_SMF.1(2)	Specification of Management Functions (Audit Record Generation)	None
FMT_SMF.1(3)	Management of TSF data (Cryptographic Key Data)	FMT_SMR.1
FPT_TST_EXP.1	TSF Testing	None
FPT_TST_EXP.2	TSF Testing of Cryptographic Modules	None

5.2.1.1 FAU_GEN.1-NIAP-0410 Audit Data Generation

FAU_GEN.1.1-NIAP-0410 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events listed in Table 9;

Table 9 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1-NIAP-0410	None	None
FCS_BCM_EXP.1	None	None
FCS_CKM_EXP.2	Error(s) detected during cryptographic key transfer	None
FCS_CKM.4	Destruction of a cryptographic key	None
FCS_COP_EXP.1	None	None
FCS_COP_EXP.2	None	None
FDP_IFC.1	Dropping a packet that fails to satisfy the Wireless Encryption Policy	MAC address of source and destination devices
FDP_IFF.1-NIAP-0407	None	None
FDP_RIP.1	None	None
FMT_SMF.1(1)	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_SMF.1(2)	Start or Stop of audit record generation	None
FMT_SMF.1(3)	Changes to the cryptographic key data	None – the TOE **SHALL NOT** record cryptographic keys in the audit log.
FPT_TST_EXP.1	Execution of the self test	Success or Failure of test
FPT_TST_EXP.2	Execution of the self test	Success or Failure of test

FAU_GEN.1.2-NIAP-0410 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 9 Auditable Events].

Application Note: In column 3 of the table below, "if applicable" is used to designate data that should be included in the audit record if it "makes sense" in the context of the event that generates the record.. If no other information is required (other than that listed in "a") for a particular audit event type, then an assignment of "none" is acceptable.

5.2.1.2 FCS_BCM_EXP.1 Explicit: Baseline Cryptographic Module

FCS_BCM_EXP.1.1 All cryptomodules shall be FIPS PUB 140-1/2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation.

FCS_BCM_EXP.1.2 The cryptomodule implemented shall have a minimum overall rating of FIPS PUB 140-1/2 Level 1.

Application Note: The term "cryptomodule" has specific meaning and is defined in the terminology section of this Protection Profile.

5.2.1.3 FCS_CKM_EXP.2 Explicit: Cryptographic Key Establishment

FCS_CKM_EXP.2.1 The TSF shall provide the following cryptographic key establishment technique: Cryptographic Key Establishment using Manual Loading.
The cryptomodule shall be able to accept as input and be able to output in the following circumstances [ST AUTHOR Assignment: circumstances under which the cryptomodule will output a key] accordance with a specified manual cryptographic key distribution method using FIPS-approved Key Management techniques that meets the FIPS 140-1/2 Key Management Security Levels 1, Key Entry and Output.;

Application Note: The ST author should use the assignment to detail the conditions under which key is output from the cryptomodule (for example, only during a certain type of key generation activity).

Note that this requirement mandates that cryptomodules in the TSF have the ability to perform manual key input/output, and that this capability has been through the FIPS validation process. This does not preclude the ST author from specifying additional key establishment techniques.

5.2.1.4 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a **cryptographic key zeroization method** that meets the following:[

a) The Key Zeroization Requirements in FIPS PUB 140-1/2 Key Management Security Levels 1;
b) Zeroization of all private cryptographic keys, plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete; and
c) The zeroization shall be executed by overwriting the key/critical cryptographic security parameter storage area three or more times with an alternating pattern.
d) The TSF shall overwrite each intermediate storage area for private cryptographic keys, plaintext cryptographic keys, and all other critical security parameters three or more times with an alternating pattern upon the transfer of the key/CSPs to another location.]

Application Note: Item d applies to locations that are used when the keys/parameters are copied during processing, and not to the locations that are used for storage of the keys, which are specified in items b and c. The temporary locations could include memory registers, physical memory locations, and even page files and memory dumps.

5.2.1.5 FCS_COP_EXP.1 Explicit: Random Number Generation

FCS_COP_EXP.1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved cryptomodule running in a FIPS-approved mode.

Application Note: Whenever a referenced standard calls for a random number generation capability, this requirement specifies the subset of random number generators (those that are FIPS-validated) that are acceptable. Note that the RNG does not have to be implemented in the cryptomodule that is performing the cryptographic operation. Also note that this requirement is not calling for the RNG functionality to be made generally available (e.g., to untrusted users via an API).

5.2.1.6 FCS_COP_EXP.2 Explicit: Cryptographic Operation

FCS_COP_EXP.2.1 A cryptomodule shall perform encryption and decryption using a FIPS 140-1/2 Approved algorithm operating in one or more FIPS 140-1/2 supporting minimum FIPS approved key sizes.

Application Note: The ST author should specify the algorithm used and iterate this requirement for each different algorithm. For example if AES is used the ST author should specify the operation in one or more of ECB, CBC, OFB, CFB1, CFB8, CFB128, or CTR modes supporting key sizes of 128 bits, 192 bits, or 256 bits.

5.2.1.7 FDP_IFC.1 Subset information flow control (Wireless Encryption Policy)

FDP_IFC.1.1(1) The TSF shall enforce the [Wireless Encryption SFP] on [subjects: client, access point/system; information: network packets; operations: receive packet and transmit packet].

Application Note: The encryption/decryption flag identifies a management setting on the TOE.

5.2.1.8 FDP_IFF.1-NIAP-0407 Simple Security Attributes (Wireless Encryption Policy)

FDP_IFF.1.1-NIAP-0407 The TSF shall enforce the [Wireless Encryption Policy] based on the following types of subject and information

security attributes: [encryption/decryption flag; direction of travel at the network interface]

FDP_IFF.1.2-NIAP-0407 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the encryption/decryption flag does NOT indicate that the TOE should perform encryption then all packets may pass without modification.
- If the direction of travel is from the operating system to the network interface and the encryption/decryption flag indicates the TOE should perform encryption, then the TOE must encrypt user data via FCS_COP_EXP.2.1 and if successful transmit the packet via the wireless interface.
- The direction of travel is from the network interface to the operating system and the encryption/decryption flag indicates the TOE should perform encryption then the TOE must decrypt user data via FCS_COP_EXP.2.1 and if successful pass that information to the operating system.
- [ST AUTHOR - selection: [ST AUTHOR - assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes], “no additional information flow Specified Access Point/System Policy Rules”]].

FDP_IFF.1.3-NIAP-0407 The TSF shall enforce the following information flow control rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: additional information flow control SFP rules], "no additional information flow control SFP rules"]

FDP_IFF.1.4-NIAP-0407 The TSF shall provide the following [ST AUTHOR - selection: [ST AUTHOR - assignment: list of additional SFP capabilities], "no additional SFP capabilities"]

FDP_IFF.1.5-NIAP-0407 The TSF shall explicitly authorize an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly authorize information flows], "no explicit authorization rules"]

FDP_IFF.1.6-NIAP-0407 The TSF shall explicitly deny an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly deny information flows], "no explicit denial rules"]

Application Note: The ST Author should use the selections and assignments in elements 1.2 thru 1.5 to indicate exceptions to the Wireless Encryption Policy (e.g. broadcast/management packets).

5.2.1.9 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1(1) The TSF shall be ensure that any previous information content of a resource is made unavailable upon the [ST AUTHOR - selection: allocation of the resource to, deallocation of the resource from] the following objects [network packet objects].

Application Note: This requirement ensures that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet. Similarly, TOE must ensure that the contents of previously transmitted packet be cleared from shared memory or other mechanisms (within the TSC) used to transfer packet data between the TOE and the computer in which the TOE is installed.

5.2.1.10 FMT_SMF.1(1) Specification of Management Functions[8] (Cryptographic Function)

FMT_SMF.1.1(1) The TSF shall be capable of performing the following management functions: [query and set the encryption/decryption of network packets (via FCS_COP_EXP.2) in conformance with the Wireless Encryption Policy].

Application Note: This requirement ensures that those responsible for TOE administration are able to select an encryption algorithm identified in FCS_COP_EXP.2 or no encryption for encrypting/decrypting data transmitted by the WLAN card.

5.2.1.11 FMT_SMF.1(2) Specification of Management Functions[8] (TOE Audit Record Generation)

FMT_SMF.1.1(2) The TSF shall be capable of performing the following management functions: [query, enable or disable Security Audit (FAU_GEN.1-NIAP-0410)].

Application Note: This requirement ensures that those responsible for TOE administration are able to start or stop the TOE generation of audit records

5.2.1.12 FMT_SMF.1(3) Specification of Management Functions[8] (Cryptographic Key Data)

FMT_SMF.1.1(2) The TSF shall be capable of performing the following management functions: [query, set, modify, and delete the cryptographic keys and key data in support of the Wireless Encryption Policy and enable/disable verification of cryptographic key testing].

Application Note: The intent of this requirement is to provide the ability to configure the TOE's cryptographic key(s). Configuring the key data may include: setting key lifetimes, setting key length, etc.

[8] The FMT_SMF (Specification of Management Functions) family is documented in CCIMB interpretation 65.

5.2.1.13 FPT_TST_EXP.1 TSF Testing

FPT_TST_EXP.1.1	The TSF shall run a suite of self-tests during initial start-up and upon request, to demonstrate the correct operation of the hardware portions of the TSF.
FPT_TST_EXP.1.2	The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of all TSF data except the following: audit data, [ST AUTHOR - selection: [ST AUTHOR - assignment: *other dynamic TSF data for which no integrity validation is justified*], *none*]].
FPT_TST_EXP.1.3	The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of stored TSF executable code.

Application Note: In element 1.1, only the hardware portions of the TSF need to be self-tested; this makes sense because hardware has the capability of degrading or failing over time, while software generally doesn't. TSF software integrity is addressed by element 1.3. In element 1.2, the ST author should specify the TSF data for which integrity validation is not required. While some TSF data are dynamic and therefore not amenable to integrity verification, it is expected that all TSF data for which integrity verification "makes sense" be subject to this requirement. In elements 1.2 and 1.3, the cryptographic mechanism can be the one specified in FCS_COP_EXP.2, although typically MAC or hash functions are used for integrity verification. Since this PP does not specifically require any MAC or hash functions the ST Author may iterate the FCS_COP_EXP.2

5.2.1.14 FPT_TST_EXP.2 TSF Testing of Cryptographic Modules

FPT_TST_EXP.2.1	The TSF shall run the suite of self-tests provided by the FIPS 140-1/2 cryptomodule during initial start-up (power on) and upon request, to demonstrate the correct operation of the cryptographic components of the TSF.
FPT_TST_EXP.2.2	The TSF shall be able to run the suite of self-tests provided by the FIPS 140-1/2 cryptomodule immediately after the generation of a key.

Application Note: The 2.2 element requires specific functionality IF the TOE generates cryptographic keys. This element does not require the TOE to generate keys.

5.3 TOE IT Environment Security Functional Requirements

Table 10 Security Functional Requirements for the TOE IT Environment

Functional Component		Dependencies[9]
FAU_SAA.1-NIAP-0407	Potential violation analysis	FAU_GEN.1
FAU_SAR.1	Audit Review	FAU_GEN.1
FAU_SAR.2	Restricted Audit Review	FAU_SAR.1
FAU_SAR.3	Selectable audit review	FAU_SAR.1
FAU_STG.1-NIAP-0429	Protected audit trail storage	FAU_GEN.1
FAU_STG.3	Action in case of possible audit data loss	FAU_STG.1
FIA_USB.1-NIAP-0415	User-subject Binding	FIA_ATD.1
FMT_MOF.1	Management of Security Functions Behavior	FMT_SMR.1
FMT_MTD.1	Management of TSF Data (Time TSF Data)	FMT_SMR.1
FMT_SMR.1	Security Roles	FIA_UID.1
FDP_RIP.1	Subset Residual Information Protection	None
FPT_RVM.1	Non Bypassability of the TSP	None
FPT_SEP.1	TOE IT Environment Domain Separation	None
FPT_STM.1	Reliable Time Stamps	None

5.3.1 FAU_SAA.1-NIAP-0407 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP

[9] The purpose of requirements on the IT environment is to supplement the TOE and to ensure that the TOE and the IT environment together satisfy all security objectives. In order to limit the scope of the IT environment only those IT environmental requirements that directly contribute to the satisfaction of objectives have been included in this PP. Requirements for the IT environment that are necessary simply to satisfy management guidance, audit guidance or dependency chains have not been included in this PP.

FAU_SAA.1.2-NIAP-0407 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation **of a single auditable event** or combination of [auditable events in Table 9] known to indicate a potential security violation;

b) *no additional rules*

5.3.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The **TOE IT environment** shall provide **only** the [Administrator] with the capability to read [all audit data] from the audit records.

FAU_SAR.1.2 Refinement: The TOE IT environment shall provide the audit records in a manner suitable for the **Administrator** to interpret the information.

Application Note: This requirement ensures that the TOE IT environment provides the administrator with functionality necessary for the administrator to review the audit records generated by the TOE.

5.3.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The **TOE IT environment** shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note: This requirement ensures that access to audit records generated by the TOE is limited to those authorized to view the information.

5.3.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches, sorting, ordering* of audit data based on [criteria with logical relations].

5.3.5 FAU_STG.1-NIAP-0429 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2- NIAP-0429 The TSF shall be able to *prevent* modifications to the audit records in the audit trail.

5.3.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [immediately alert the administrators by displaying a message at the local console, [selection:[assignment: other actions determined by the ST author], "none"]] if the audit trail exceeds [an Administrator-settable percentage of storage capacity].

Application Note: The ST Author should determine if there are other actions that should be taken when the audit trial setting is exceeded, and put these in the assignment. If there are no other actions, then the ST Author should select "none".

5.3.7 FIA_USB.1-NIAP-0415 User-subject binding

FIA_USB.1.1-NIAP-0415 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [authentication credentials].

5.3.8 FMT_MTD.1 Management of TSF Data (Time TSF Data)

FMT_MTD.1.1 The **TOE IT Environment** shall restrict the ability to *set* the [time and date used to form the time stamps in FPT_STM.1] to [the Administrator].

Application Note: The TOE IT environment must provide an interface for the Administrator to set the time and date.

5.3.9 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The **TOE IT Environment** shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects [network packet objects].

Application Note: This requirement ensures that the TOE IT Environment does not allow data from a previously transmitted packet to be inserted into unused areas or padding in the current packet. Since operations on requirement for the IT environment must be completed, the selection "allocation of resources to" has been made because it encompassing of the two options (e.g. a system that make the information contents of resource unavailable when the resource is freed can also claim to meet the requirement that the content of the resource be freed prior to reallocation).

5.3.10 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The **TOE IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.3.11 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TOE IT environment shall restrict the ability to *determine the behavior* of the functions:

[encryption/decryption of network packets (FMT_SMF.1(1), FMT_SMF.1(3)), audit (FMT_SMF.1(2))] to [the administrator].

Application Note: The environment provides a mechanism to restrict access to the management of the card.

5.3.12 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The **TOE IT environment** shall maintain the role [Administrator].

FMT_SMR.1.2 The **TOE IT environment** shall be able to associate users with roles.

Application Note: The TOE IT environment provides support for the administrative role that is used to administer the TOE. In some environments, the administrative role will be fulfilled by the end user (e.g. a laptop computer). However, other environments (e.g. a multi-user system), the administrative role will be provided by someone other than the end user.

5.3.13 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The **TOE IT environment** shall be able to provide reliable time **and date** stamps for **the TOE and** its own use.

Application Note: The TOE IT environment must provides time stamps that are used by the TOE.

5.3.14 FPT_SEP.1 TOE IT Environment Domain Separation

FPT_SEP.1.1 The **TOE IT environment** shall maintain a security domain that protects **the TOE and the TOE IT environment** from interference and tampering by untrusted subjects initiating actions through the **IT environment kernel interface**.

FPT_SEP.1.2 The TOE IT environment shall enforce separation between the security domains of subjects in the **TOE IT environment's** Scope of Control.

5.4 TOE Security Assurance Requirements

The TOE security assurance requirements, summarized in

Table 11, identify the management and evaluative activities required to address the threats and policies identified in section 3 of this protection profile. Section 5 provides a justification for the chosen security assurance requirements and the selected EAL 2 assurance level.

Table 11: TOE Assurance Requirements

Assurance Class	Assurance Components
Configuration Management	Authorization controls (ACM_CAP.2 as modified by NIAP Interpretation I-0412) TOE CM Coverage (ACM_SCP.1)
Delivery and Operations	Delivery procedures (ADO_DEL.1) Installation, generation, and start-up procedures (ADO_IGS.1)
Development	Informal functional specification (ADV_FSP.1) Security enforcing high-level design (ADV_HLD.1) Informal correspondence demonstration (ADV_RCR.1)
Guidance documents	Administrator guidance (AGD_ADM.1) User guidance (AGD_USR.1)
Life-Cycle Support	Flaw Remediation (ALC_FLR.2)
Tests	Analysis of coverage (ATE_COV.2) Functional testing (ATE_FUN.1) Independent testing—sample (ATE_IND.2)
Vulnerability Assessment	Examination of guidance (AVA_MSU.1) Strength of TOE security function evaluation (AVA_SOF.1) Developer vulnerability analysis (AVA_VLA.1)

6. Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined in Section 4 and Section 5, respectively. Additionally, this section describes the rationale for not satisfying all of the dependencies and the rationale for the strength of function (SOF) claim.
Table 12 illustrates the mapping from Security Objectives to Threats and Policies.

6.1 Rationale for Security Objectives

Table 12: Security Objectives to Threats and Policies Mappings

Threat/Policy	Objectives Addressing the Threat	Rationale
T.ACCIDENTAL_ADMIN_ ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	O.ADMIN_GUIDANCE (ADO_DEL.2, ADO_IGS.1, AGD_ADM.1, AGD_USR.1, AVA_MSU.2) help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure. OE.MANAGE (FAU_SAR.1) ensures that the administrator can view security relevant audit events.
T.ACCIDENTAL_CRYPTO_C OMPROMISE A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or deleted), thus compromising the cryptographic mechanisms and the date protected by those mechanisms.	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.SELF_PROTECTION The TOE IT environment will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through its their interfaces.	O.RESIDUAL_INFORMATION and OE.RESIDUAL_INFORMATION (FDP_RIP.1) contribute the mitigation of this threat by ensuring that neither the TOE or the TOE IT environment will insert critical data (including data related to encryption) and executable code as padding in network packet objects. In addition, FCS_CKM_EXP.2 and FCS_CKM.4 ensure that FIPS 140-1/2 procedures are followed when cryptographic keys are handled and destroyed. OE.SELF_PROTECTION (FPT_SEP.1 and FDP_RVM.1) ensure that the TOE IT environment will protect the TOE and itself from users.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.POOR_DESIGN Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.DOCUMENTED_ DESIGN The design of the TOE is adequately and accurately documented. O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly. O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.DOCUMENTED_DESIGN (ADV_FSP.1, ADV_HLD.1, ADV_RCR.1) counters this threat, to a degree, by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increase the chances that accidental design errors will be discovered. ADV_RCR.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification. O.CONFIGURATION_IDENTIFICATIO N (ACM_CAP.2, ACM_SCP.1, ALC_FLR.2) plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. O.VULNERABILITY_ANALYSIS_TEST (AVA_VLA.1, AVA_SOF.1) ensure that the TOE has been analyzed for obvious vulnerabilities and that any vulnerabilities found have been removed or otherwise mitigated, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE claiming conformance to this PP.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.POOR_IMPLEMENTATION Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly. O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATIO N (ACM_CAP.2, ACM_SCP.1, ALC_FLR.2) plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked. O.PARTIAL_FUNCTIONAL_TESTING (ATE_COV.1, ATE_FUN.1, ATE_IND.2) ATE_COV.1 ensures that the developers testing of the TOE is sufficiently address all TOE Security Functional requirements. ATE_IND.2 contributes to removing this threat by ensuring that the security relevant portions of the TOE have been tested against the security functional requirements. O.VULNERABILITY_ANALYSIS_TEST (AVA_VLA.1, AVA_SOF.1) ensure that the TOE has been analyzed for obvious vulnerabilities and that the TOE resistant casually mischievous users, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE claiming conformance to this PP.
T.POOR_TEST Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.	O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.PARTIAL_FUNCTIONAL_TESTING contributes to removing this threat by ensuring that the security relevant portions of the TOE have been tested against the security functional requirements. O.CORRECT_ TSF_OPERATION (FPT_TST_EXP.1, FPT_TST_EXP.2) ensure that users can verify the continued correct operation of the TOE after it has been installed in its target environment. O.VULNERABILITY_ANALYSIS_TEST (AVA_VLA.1) ensure that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION (FDP_RIP.1(1)) The TOE contributes to the mitigation of this threat by ensuring that network packet objects are cleared prior to use. In addition, FCS_CKM_EXP.2 and FCS_CKM.4 ensure that FIPS 140-1/2 is followed and objects used to store cryptographic keys is overwritten when those keys are no longer needed. OE.RESIDUAL_INFORMATION (FDP_RIP.1(IT 2)) contribute the mitigation of this threat by ensuring that neither the TOE or the TOE IT environment will insert critical data (including data related to encryption) and executable code as padding in network packet objects.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.TSF_COMPROMISE A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.SELF_PROTECTION The TOE IT environment will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through its their interfaces.	O.MANAGE (FMT_.1(1), FMT_.1(2), FMT_.1, FMT_MSA.3, FMT_.1(FMT_.1()) and OE.MANAGE (FMT_MOF.1, FMT_MTD.1) mitigate this threat by restricting access to administrative functions and TSF data to the administrator. O.RESIDUAL_INFORMATION (FDP_RIP.1, FCS_CKM.4)) and OE.RESIDUAL (FDP_RIP.1(IT 2)) contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed. OE.SELF_PROTECTION (FPT_SEP.2, FPT_RVM.1) requires that the TOE IT environment be able to protect itself and the TOE from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables.

Threat/Policy	Objectives Addressing the Threat	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events. O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. OE.TIME_STAMPS The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. OE.TOE_ACCESS The TOE IT environment will provide mechanisms that control a user's logical access to the TOE.	O.AUDIT_GENERATION (FAU_GEN.1-NIAP-0410) ensure that the TOE is capable of generating records of audit events. O.MANAGE (FMT_SMF.1(2)) ensures that the administrator can enable or disable the audit function. OE.MANAGE (FAU_SAR.1, FAU_SAR.2, FMT_MOF.1) ensure that the administrator can review the audit event log restricts access to this information to the administrator. OE.TIME_STAMPS (FPT_STM.1, FMT_MTD.1) plays a role in supporting this policy by requiring the TOE IT environment provide a reliable time stamp (configured locally by the Administrator or via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. OE.TOE_ACCESS (FMT_SMR.1 and FIA_USB) contributes to the mitigation of this threat by ensuring that the TOE IT environment provides an administrative role and provides a mechanism to identify processes acting on behalf of the administrator.
P.CRYPTOGRAPHY Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).	O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-1/2 validated cryptographic services.	O.CRYPTOGRAPHY (FCS_BCM_EXP.1, FCS_CKM_EXP.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2, FDP_IFC.1(2), FDP_IFF.1-NIAP-0407) satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. O.RESIDUAL_INFORMATION (FCS_CKM_EXP.2, FCS_CKM.4) satisfies this policy by ensuring that cryptographic data are cleared according to FIPS 140-1/2.

6.2 Additional Rationale for Security Objectives in the TOE IT Environment

Three of the security objectives for the TOE are simply restatements of an assumption found in Section 3. Therefore, these three objectives for the environment, OE.BASIC_ROBUSTNESS_OS, OE.NO_EVIL and OE.PHYSICAL, trace to the assumptions trivially.

Of these three, only OE.BASIC_ROBUSTNESS_OS bares further discussion. This assumption has been included in the PP because the TOE is not expected to address all of the threats and policies defined in a basic robustness environment. As such, the eventual user of the TOE must take additional steps to ensure the environment in which the TOE is used, has been hardened to the basic robustness level. This objective and its corresponding assumption should NOT be construed to allow the TOE IT environment to satisfy objectives or requirements levied on the TOE.

The remainder of the security objectives for the IT environment have been included in this Protection Profile in order to support the TOE security functions. The rationale support is documented in
Table 12 along with the rationale for security objectives for the TOE.

6.3 Rationale for TOE Security Requirements

Table 13: Rationale for TOE Security Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	ADO_DEL.1 AGD_ADM.1 AVA_MSU.1 ADO_IGS.1 AGD_USR.1	ADO_DEL.1 ensures that the administrator has the ability to begin their TOE installation with a *clean* (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE. The ADO_IGS.1 requirement ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. The AGD_ADM.1 requirement ensures that the developer provides the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces used in managing the TOE, and any security parameters that are configurable by the administrator. The

Objective	Requirements Addressing the Objective	Rationale
		documentation also provides a description of how to setup and review the auditing features of the TOE. The AGD_USR.1 is intended for non-administrative users. If the TOE provides facilities/interfaces for this type of user, this guidance will describe how to use those interfaces securely. AVA_MSU.1 ensures that the guidance documentation can be followed unambiguously to ensure the TOE is not mis-configured in an insecure state due to confusing guidance.
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events.	FAU_GEN.1-NIAP-0410	FAU_GEN.1-NIAP-0410 defines the set of events that the TOE must be capable of recording. This requirement ensures that the Security Administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds.
O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.	ACM_CAP.2 ACM_SCP.1 ALC_FLR.2	ACM_CAP.2 contributes to this objective by requiring the developer have a configuration management plan that describes how changes to the TOE and its evaluation deliverables are managed. ACM_SCP.1 is necessary to define the items that must be under the control of the CM system. This requirement ensures that the TOE implementation representation, design documentation, test documentation (including the executable test suite), user and administrator guidance, and CM documentation are tracked by the CM system. ALC_FLR.2 plays a role in satisfying this objective by requiring the developer to have procedures that address flaws that have been discovered in the product, either through developer actions (e.g., developer testing) or those discovered by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.
O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FPT_TST_EXP.1 FPT_TST_EXP.2	FPT_TST_EXP.1 is necessary to ensure the correctness of the TSF software and TSF data. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies. The FPT_TST_EXP.2 functional

Objective	Requirements Addressing the Objective	Rationale
		requirement has been included to address the critical nature and specific handling of the cryptographic related TSF data. Since the cryptographic TSF data has specific FIPS PUB requirements associated with them it is important to ensure that any fielded testing on the integrity of these data maintains the same level of scrutiny as specified in the FCS functional requirements.
O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-1/2 validated cryptographic services.	FCS_BCM_EXP.1 FCS_CKM_EXP.2 FCS_CKM.4 FCS_COP_EXP.1 FCS_COP_EXP.2 FDP_IFC.1 FDP_IFF.1-NIAP-0407	The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-1/2 validation. FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested. FCS_CKM_EXP.2 Cryptographic Key Handling and Storage requires that FIPS PUB 140-1/2 be satisfied when performing key entry and output. FCS_CKM.4 mandates the standards (FIPS 140-1/2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. FCS_COP_EXP.1 requires that for any cryptomodule implemented in the TOE use a FIPs approved random number generator when it is necessary to generate random numbers. FCS_COP_EXP.2 requires that for data decryption and encryption that the NIST approved Advanced Encryption Standard - Rijndael (AES) algorithm be used, and that the algorithm meets the FIPS PUB 140-1/2, FIPS PUB 197 standard. FDP_IFC.1 and FDP_IFF.1-NIAP-0407 identify the policy that the TOE must implement to encrypt/decrypt user data.
O.DOCUMENTED_ DESIGN The design of the TOE is adequately and accurately documented.	ADV_FSP.2 ADV_HLD.1 ADV_RCR.1	ADV_FSP.1 requires that the security relevant interfaces to the TSF be completely specified. In this TOE, a complete specification of the network interface is critical in understanding what functionality is presented to untrusted users and how that functionality fits into the enforcement of security policies. Having a complete understanding of what is

Objective	Requirements Addressing the Objective	Rationale
		available at the TSF interface allows one to analyze this functionality in the context of design flaws. ADV_HLD.1 requires that a high-level design of the TOE be provided. This level of design describes the architecture of the TOE in terms of subsystems. It identifies which subsystems are responsible for making and enforcing security relevant (e.g., anything relating to an SFR) decisions and provides a description, at a high level, of how those decisions are made and enforced. Having this level of description helps to provide a general understanding of the TOE and how it functions. The ADV_RCR.1 is used to ensure that the decomposition of the TOE's design are consistent with one another. This is important, since design decisions that are analyzed and made at one level (high level design) that are not correctly or completely realized at a lower level (the functional specification) may lead to a design flaw. This requirement helps in the design analysis to ensure design decisions are realized at across the design. A complete and accurate description of the TOE design is critical to understanding the TOE design. It is this understanding, gained is from the design analysis, which the evaluator relies upon during testing and vulnerability analysis activities.
O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE.	FMT_SMF.1(1) FMT_SMF.1(2) FMT_SMF.1(3)	The FMT requirements are used to satisfy the management objective, as well as other objectives that specify the control of functionality. The requirement's rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions. FMT_SMF.1(1) and FMT_SMF.1(3)ensures that the administrator has the ability to control the use of encryption when the TOE is communicating with external systems. FMT_SMF.1(2) provides the administrator with control of the TOE audit record generation mechanism.
O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional	ATE_COV.1 ATE_FUN.1 ATE_IND.2	In order to satisfy O.FUNCTIONAL_TESTING, the ATE class of requirements is necessary. ATE_FUN.1 requires the developer to provide the necessary test documentation to allow for an independent analysis of the developer's security functional test coverage. In addition, the developer

Objective	Requirements Addressing the Objective	Rationale
requirements.		must provide the test suite executables and source code, which the evaluator uses to independently verify the vendor test results and to support of the test coverage analysis activities. ATE_COV.1 requires the developer to provide a test coverage analysis that demonstrates the extent to which the TSFI are tested by the developer's test suite. This component also requires an independent confirmation of the extent of the test suite, which aids in ensuring that correct security relevant functionality of a TSFI is demonstrated through the testing effort. ATE_IND.2 requires an independent confirmation of the developer's test results, by mandating a subset of the test suite be run by an independent party. This component also requires an independent party to craft additional functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful completion of these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.
O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	FDP_RIP.1 FCS_CKM_EXP.2 FCS_CKM.4	FDP_RIP.1 is used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data). FCS_CKM_EXP.2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1, in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately cleared as opposed to waiting until the memory is reallocated to another subject. FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.
O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VLA.1 AVA_SOF.1	AVA_VLA.1 requires the developer to perform a search for obvious vulnerabilities in all the TOE deliverables. The developer must then document the disposition of those obvious vulnerabilities. The evaluator then builds upon this analysis during vulnerability testing. This component provides the confidence that obvious security flaws have been

Objective	Requirements Addressing the Objective	Rationale
		either removed from the TOE or otherwise mitigated. AVA_SOF.1 requires that any permutational or probabilistic mechanism in the TOE be analyzed be found to be resistant to attackers possessing a "low" attack potential. This provides confidence that security mechanisms vulnerable to guessing type attacks are resistant to casual attack.

6.4 Rationale for TOE IT Environment Security Requirements

Table 14: Rationale for Requirements on the TOE IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FAU_SAR.1 FAU_SAR.2 FIA_USB.1 FMT_MOF.1 FMT_MTD.1 FMT_SMR.1	FMT_SMR.1 ensures that the TOE IT environment provides an administrative role that may be used to manage both the TOE and the IT environment. FIA_USB.1 ensures that the TOE IT environment includes a mechanism to associate processes with roles. This ensures that both the TOE and its IT environment can identify FAU_SAR.1 ensures that the IT environment provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the Audit Administrator can construct a sequence of events provided the necessary events were audited). FAU_SAR.2 ensures that the TOE IT environment will be capable of limit access to TOE audit records to only those with those users authorized to review them. FMT_MOF.1 ensures that the TOE IT environment limits access to TSF management functions to the administrator. FMT_MTD.1 ensures that the IT environment provides facilities to manage the time stamp mechanism.
OE.NO_EVIL Administrators are non-hostile, appropriately trained and follow all administrator guidance.	AGD_ADM.1	The AGD_ADM.1 requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a

Objective	Requirements Addressing the Objective	Rationale
		description of how to setup and review the auditing features of the TOE.
OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the TOE environment.	A.Physical	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment. Therefore, an explicit requirement is not necessary.
OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	FDP_RIP.1	FDP_RIP.1 ensures that the TOE IT environment provides same protections for residual information in a network packet that the TOE will provide. This ensures that neither the TOE nor the TOE IT environment will allow data from previously transmitted packets to be insert into new packets.
OE.SELF_PROTECTION The TOE IT environment will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through its their interfaces.	FPT_RVM.1 FPT_SEP.1	FPT_SEP.1 ensures that the TOE IT environment provides a domain that protects itself and the TOE from untrusted users. Since the TOE is a component of a larger system, it cannot protect itself and must rely on the IT environment. If the IT environment cannot protect both itself and the TOE, then the TOE cannot be relied upon to enforce its security policies. The inclusion of FPT_RVM.1 ensures that the TOE is able to make policy decisions on all packets passing between the TOE IT environment and the Wireless LAN. Without this non-bypassability requirement, the TOE could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to Wireless LAN regardless of the defined policies. Since the TOE is a component of a larger system, the TOE by itself cannot enforce FPT_RVM.
OE.TIME_STAMPS The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	FPT_MTD.1 FPT_STM.1 FMT_SMR.1	FPT_STM.1 ensures that the IT environment provides a time stamp mechanism that may be used to synchronize audit events. FMT_MTD.1 ensures that the IT environment provides facilities to manage the time stamp mechanism and limits access to the time stamp mechanism to the administrator FMT_SMR.1 ensures that the TOE IT environment provides an administrative role that may be used to manage both the TOE and the IT environment.
OE.TOE_ACCESS The TOE IT environment will provide mechanisms that control a user's logical access to the TOE.	FMT_SMR.1 FIA_USB.1	FMT_SMR.1 ensures that the TOE IT environment provides an administrative role that may be used to manage both the TOE and the IT environment. FIA_USB.1 ensures that the TOE IT environment includes a mechanism to associate processes with roles. This ensures that both the TOE and its IT environment can identify

6.5 Rationale for Assurance Requirements

EAL2 augmented was chosen to ensure a confidence in security services used to protect information in a Basic Robustness Environment. The assurance selection was based on:

- recommendations documented in the GIG; and
- the postulated threat environment.

The EAL definitions in Part 3 of the CC were reviewed and the *Basic Robustness Assurance Package* (Evaluation Assurance Level (EAL) 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of Guidance).) was believed to best achieve this goal. The sponsor concluded that EAL2 augmented is applicable since this PP addresses circumstances where users require a basic level of independently assured security in commercial products. This level of assurance is commensurate with low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This collection of assurance requirements require TOE developers to gain assurance from good software engineering development practices which, do not require substantial specialist knowledge, skills, and other resources. Rationale for individual assurance requirements is provided in Table 13.

The Government's guidance in the GIG was consulted and found to also support the chosen assurance package. Specifically, the GIG states that basic robustness security services and mechanisms provide t the DoD minimum and require good assurance security design as specified in EAL1 or greater.

The postulated threat environment specified in Section 3 of this PP was used in conjunction with the Information Assurance Technical Framework (IATF) Robustness Strategy guidance to derive the chosen assurance level.

These three factors were taken into consideration and the conclusion was that the basic robustness assurance package was the appropriate level of assurance.

6.6 Rationale for Not Satisfying All Dependencies

Each functional requirement, including explicit requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. ting the dependency in this PP.

Table 15 identifies the functional requirement, its correspondent dependency and the analysis and rationale for not supporting the dependency in this PP.

Table 15: Unsupported Dependency Rationale

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FCS_CKM_EXP.2	FCS_CKM.1	In the context of FCS_CKM_EXP.2, the FCS_CKM.1 requirements allows the PP/ST author to specify key generation standards for cryptographic keys used by

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
		the TOE. Since the WLAN client TOE is not expected to generate keys, this requirement has been omitted. Note: this PP specifies manual key entry.
FCS_CKM_EXP.2	FMT_MSA.2	The FMT_MSA.2 requirement simply states that "The TSF shall ensure that only secure values are accepted for security attributes". In the context of FCS_CKM_EXP.2, it is not clear what security attributes/secure values are associated with handling cryptographic keys. Therefore this requirement has been omitted.
FDP_IFC.1	FMT_MSA.3	The FDP_IFC.1 requirement specifies the Wireless Encryption Policy. The FMT_MSA.3 allows the PP author to specify secure default values for that policy. However, since the FMT_SMF.1(1) and FMT_SMF.1(3) provides the ability to set the policy. The ability to set a secure initial default value (e.g. decrypt by default) is not necessary.
FIA_USB.1	FIA_ATD.1	This dependency is on a requirement for the TOE IT environment. The purpose of requirements on the IT environment is to supplement the TOE and to ensure that the TOE and the IT environment together satisfy all security objectives. In order to limit the scope of the IT environment only those IT environmental requirements that directly contribute to the satisfaction of objectives have been included in this PP. Requirements for the IT environment that are necessary simply to satisfy management guidance, audit guidance or dependency chains have not been included in this PP. In the context of FIA_USB, the FIA_ATD dependency is used to specify user security attributes used to enforce the TSP. Since FIA_USB is specified for the TOE IT environment, FIA_ATD would also need to be specified for the TOE IT environment. However, including this requirement in the IT environment does not directly contribute to the satisfaction of any TOE objectives therefore it has been omitted.
FMT_SMR.1	FIA_UID.1	This dependency is on a requirement for the TOE IT environment. The purpose of requirements on the IT environment is to supplement the TOE and to ensure that the TOE and the IT environment together

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
		satisfy all security objectives. In order to limit the scope of the IT environment only those IT environmental requirements that directly contribute to the satisfaction of objectives have been included in this PP. Requirements for the IT environment that are necessary simply to satisfy management guidance, audit guidance or dependency chains have not been included in this PP. In the context of FMT_SMR the FIA_UID requirement is used to specify the action available to a user that has not been identified. It is expected that any role specified supported the IT environment would require both identification and authentication components. However, including this requirement in the IT environment does not directly contribute to the satisfaction of any TOE objectives therefore it has been omitted.

6.7 Rationale for Strength of Function Claim

Part 1 of the CC defines "strength of function" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this PP. SOF-basic states, "a level of the TOE strength of function where analysis shows that the function provides adequate protection casual breach of TOE by attackers possessing a low attack potential." The rationale for choosing SOF-basic was to be consistent with the TOE objective O.VULNERABILITY_ANALYSIS and assurance requirements included in this PP. Specifically, AVA_VLA.1 requires that the TOE be resistant obvious vulnerabilities, this is consistent with SOF-basic, which is the lowest strength of function metric. Consequently, security functions with probabilistic or permutational mechanisms chosen for inclusion in this PP were determined to adequately protect information in a Basic Robustness Environment. Similarly, probabilistic or permutational security functions included in any ST claiming conformance to this PP, must also meet an SOF Basic metric.

6.8 Rationale for Explicit requirements

Table 16 presents the rationale for the inclusion of the explicit requirements found in this PP.

Table 16: Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale

Explicit Requirement	Identifier	Rationale
FCS_BCM_EXP.1	Baseline cryptographic module	This explicit requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation. This is explicit requirement is also necessary because it describes requirements for a FIPS 140-1/2 validated cryptomodule rather that the entire TSF.
FCS_CKM_EXP.2	Cryptographic Key Establishment	This explicit requirement is necessary to because the
FCS_CKM_EXP.2	Cryptographic key handling and storage	This is explicit requirement is necessary because it describes requirements for a FIPS 140-1/2 validated cryptomodule rather that the entire TSF.
FCS_COP_EXP.1	Random number generation	This explicit requirement is necessary since the CC cryptographic operation components are focused on specific algorithm types and operations requiring specific key sizes.
FCS_COP_EXP.2	Cryptographic Operation (Encryption/Decryption using AES)	This is explicit requirement is necessary because it describes requirements for a FIPS 140-1/2 validated cryptomodule rather that the entire TSF.

7. References

1. US Government Wireless Access System for Basic Robustness Environments Protection Profile, Version *0.95.*

2. Common Criteria for Information Technology Security Evaluation, Version 2.1. CCIMB-99-021, 032, 033. August 1999.

3. Global Information Grid (GIG) Policy 6-8510, Information Assurance Guidance, 16 June 2000.
4. Common Methodology for Information Technology Security Evaluation, Version 1.0, CEM-99/045, August 1999.

Appendix A. Acronyms

CC	Common Criteria
CM	Configuration Management
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GIG	Global Information Grid
HARA	High-Assurance Remote Access
ISSE	Information System Security Engineers
IT	Information Technology
OSP	
PKI	Public Key Infrastructure
PP	Protection Profile
PUB	Publication
RF	Radio Frequency
SBU	Sensitive But Unclassified
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SoF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WLAN	Wireless Local Area Network